U.S. Department of Justice

United States Marshals Service

EX PARTE OR LATE FILED

Director

600 Army Navy Drive
Arlington, VA 22202-4210

DEC 7 1998

Ms. Magalie R. Salas
Secretary
Federal Communications Commission
1919 M Street, NW
Washington, D.C. 20544

Re: Ex Parte Presentation Regarding *In the Matter of Communications Assistance for Law Enforcement Act,* Notice of Proposed Rulemaking, Public Notice, CC Docket No. 97-213, DA 98-762, (rel. April 20, 1998)

Dear Ms. Salas:

Pursuant to Section 1.1206(B)(1) of the Commission's rules,[1] this letter is to advise the Federal Communications Commission of the importance of implementing CALEA in an expeditious manner in connection with the above-referenced rulemaking proceeding. Enclosed are copies of the letters I have sent to each Commissioner of the Federal Communications Commission. In addition, I have written ex parte communications discussing the importance of acquiring the nine assistance capability requirements that the Department of Justice has sought in the Petition for Rulemaking and its additional filings on this issue.

Any questions regarding this notice should be addressed to me at (202) 307-9001.

Sincerely,

Eduardo Gonzalez
Director

Enclosure(s)

[1] 47 C.F.R. § 1.1206(B)(1)

No. of Copies rec'd 0
List A B C D E

Re: Request for Meeting in Support of Communications Assistance for Law Enforcement Act.

cc: Julius Knapp, Office of Engineering and Technology
Charles Iseman, Office of Engineering and Technology
Rodney Small, Office of Engineering and Technology
David Wye, Wireless Telecommunication Bureau

CAPABILITIES MISSING FROM INDUSTRY'S INTERIM STANDARD J-STD-025

The following 9 capabilities, which the Department of Justice has determined are within the scope of CALEA and to be consistent with the underlying electronic surveillance law, were identified by law enforcement as necessary to support electronic surveillance, and are missing from industry's interim standard, J-STD-025. Industry based J-STD-025 requirements on the extremely limiting assumption that "call-identifying information" meant only telephone numbers.

Capability #1: Content of conference calls. Law enforcement needs to receive all conversations between two or more parties supported by a subject's conference service, whether the subject is on the line or not. This supports the primary intent of a Title III interception to access and deliver *all* communications supported by the subject's "equipment, facilities, or services." J-STD-025 only requires communications from a conference call to be delivered to law enforcement when the subject's *terminal* is connected to the conference. (Criminal subjects very often use *other* terminals to call their *own* telephone number to use their services.)

Capability #2: Party Hold, Party Join, and Party Drop Messages. These messages identify all parties in a subject's conference at any time during the conference. Knowing when each participant of a call joins or departs the call enables law enforcement to know the source and recipient of each communication within the call. Without those messages, law enforcement will not know when a party joins or leaves a conference. Law enforcement will not know if the subject alternates between calls. Law enforcement will not know which party said or heard a particular portion of a conversation under surveillance. By providing incomplete call-identifying information, the industry will deny evidence that parties remained on, or departed from the call after they first joined. The lack of such evidence allows doubt to be raised as to whether a party participated in subsequent communications during the call and jeopardizes that evidence.

Capability #3: Access to subject-initiated dialing and signaling. Law enforcement needs to know *all* of the subject's input to the network (e.g., dialing) throughout each call to understand how the subject directs the communications. Without such information, law enforcement will not know what keys a subject pressed to control calls to or from the subject's service. Law enforcement will be unable to testify as whether the subject was still involved in the call, in what fashion the subject was involved in the call, and how the subject controlled his services related to the call or separate from the call.

Capability #4: Notification Messages for in-band and out-of-band signaling. Law enforcement needs to know what network information is sent to the subject or associates from the subject's service throughout each call. Such information tells the subject and law enforcement whether a particular directive by the subject or associate results in the establishment of a call, a redirection or modification of a call, or how the call terminates or releases. Law enforcement will not know what information the network provides the subject about calls to associates, and will not know what information the subject's service provides to associates. That information often causes the subject or associate to take a particular course of action which may prove critical to law enforcement's understanding as to why and how events took place.

Capability #5: Timely delivery of call data. Law enforcement needs to be able to associate *call data* (e.g., numbers dialed) with *call events*. Furthermore, call data must be delivered in time to be useful during emergency situations. Currently, J-STD-025 places *no* requirements on when call data is to be delivered. Law enforcement is requesting that call data be delivered to law enforcement within a specific time after a call event comparable to the speed with which other signaling messages are sent in the public network. Without any such requirement, law enforcement will not be able to clearly associate call data with the correct call, raising doubts about the validity of the evidence. Timely delivery of data will also permit quick reaction to situations where the lives are threatened of law enforcement agents, innocent victims, or even the criminal themselves. Life-saving action may be delayed until call data can identify the party involved and their whereabouts.

Capability #6: Surveillance Status Message. This message indicates that the interception software is working correctly, and is accessing the subject, rather than an innocent subscriber. It will also confirm that the path over which data messages are sent is still operational. Without this capability, law enforcement will not know when the surveillance is turned on or off, or if it has failed. Law enforcement will not be able to verify that the subject is being monitored until a call is received, leaving open the possibility that evidence is lost. Providing this message will enable law enforcement to quickly correct any faults in the implementation of an interception.

Capability #7: Feature Status Message. This message reports when a subject's features (e.g., call forwarding number) change, even when the subject modifies them from another phone. Law enforcement's capability to intercept may not match the subject's capability, and evidence will be lost if lines are unavailable. Manual methods will not be cost-effective for either law enforcement or the carriers. Cellular carriers in particular already have a need to pass such information between a home and visited switch and have already incorporated such a capability in their signaling messages.

Capability #8: Continuity Check. A continuity check capability will verify that a phone line between the carrier and law enforcement works. The intent is to enable law enforcement to know when a communications delivery circuit has failed. This is different from a delivery circuit being available for service but idle. Uncorrected failures will mean loss of evidence.

Capability #9: Dialed Digit Extraction. Extracting dialed digits from the communications path and delivery of all dialed digits over a *single line* to law enforcement results in a cost-effective use of circuits for both law enforcement and carriers. Under the current standard, calls which are set up in steps through multiple carriers, such as toll-free and collect calling numbers, law enforcement will not get all digits on one line. The initial dialing will be delivered as data, while the industry has proposed delivering dialing to subsequent carriers by providing the call content. Law enforcement does not want to lease two different lines to receive only dialing information and does not want the responsibility of separating dialed digits from content, which prompts privacy concerns.

CALEA STATUTORY AUTHORITY FOR PUNCH LIST CAPABILITIES

Punch List Capability	Statutory Cite	Statutory Language
1. Contents of Subject-initiated conference calls	103(a)(1)	"All wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier."
2. Party hold, Join, Drop	102(2)	"Call-identifying information" because it "identifies the * * * direction [and] destination * * * of each communication" involved in a multi-party call.
3. Access to Subject-initiated dialing & signaling	102(2)	"Call-identifying information" because it identifies the "direction" and "destination" of the subject's communications.
4. In-band & Out-of-band Signaling (Notification Message)	102(2)	"Call-identifying information" includes "signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber."
5. Timely delivery of call-identifying information	103(a)(2)(A),(B)	Carriers are obligated to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission" of the communication to which it pertains, or "at such later time as may be acceptable to the government." Carriers also required that call identifying information be made available "in a manner that allows it to be associated with the communication to which it pertains."
6. Surveillance Status Message	103(a)	Carrier "shall ensure" that its equipment is capable of providing law enforcement with communications and call-identifying information.
7. Feature Status Message	103(a)	Carrier "shall ensure" that its equipment is capable of providing law enforcement with communications and call-identifying information.
8. Continuity Check (C-Tone)	103(a)	Carrier "shall ensure" that its equipment is capable of providing law enforcement with communications and call-identifying information.
9. Post-cut-through dialing	102(2), 103(a)(2)	Post-cut-through dialed digits that complete a call are "dialing or signaling information" that identifies the "destination" of the call. Failure to provide this information conflicts with the carrier's obligation to "isolate and enable the government * * * to access call-identifying information that is reasonably available to the carrier."

DESCRIPTION OF PUNCH LIST CAPABILITIES

Punch List Capability	Description	Availability
1. Contents of Subject-initiated conference calls	Capability would enable law enforcement access to content of conference calls supported by the subject's service (including the call content of parties on hold).	Impediment leading to CALEA. Conference calling was not available when original electronic surveillance laws were considered.
2. Party hold, Join, Drop	Message would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, whether a party is on hold, has joined or has been dropped from the conference call.	Impediment leading to CALEA. Subscriber control of calls was not available when original electronic surveillance laws were considered.
3. Access to Subject-initiated dialing & signaling	Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features. (Examples include the use of flash-hook, and other feature keys).	All subject-initiated dialing & signaling was available to law enforcement when original electronic surveillance laws were considered.
4. In-band & Out-of-band Signaling (Notification Message)	A message would be sent to law enforcement when a subject's service sends a tone or other network message to the subject or associate. This can include notification that a line is ringing, or busy.	All signaling associated with a subject was available to law enforcement when original electronic surveillance laws were considered.
5. Timely delivery of call-identifying information	Information necessary to correlate call identifying information with the call content of a communications interception.	Impediment leading to CALEA. Timely delivery of call-identifying information was available to law enforcement when original electronic surveillance laws were considered.
6. Surveillance Status Message	Message that would provide the verification that an interception is still functioning on the appropriate subject.	Available to law enforcement when original electronic surveillance laws were considered.
7. Feature Status Message	Message that would provide affirmative notification of any change in a subject's subscribed-to features.	Impediment leading to CALEA. Subscriber "features" were not nearly as sophisticated when original electronic surveillance laws were considered.
8. Continuity Check (C-Tone)	Electronic signal that would alert law enforcement if the facility used for delivery of call content interception has failed, or lost continuity.	Available to law enforcement when original electronic surveillance laws were considered.
9. Post-cut-through dialing	Information would include those digits dialed by a subject after the initial call setup is completed.	Available to law enforcement when original electronic surveillance laws were considered.